Kaspersky Industrial Cybersecurity Conference 2021

Сенсация под микроскопом: Вивисекция первого реального кибериммунного устройства для IIoT - KISG 100 на KasperskyOS

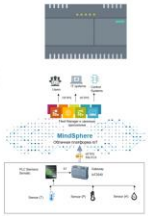
Андрей Суворов,
Максим Карпухин,
НПО Адаптивные промышленные технологии (АПРОТЕХ)

kaspersky

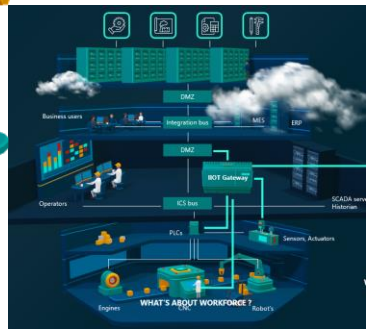
Сочи Пост-олимпийский

Идея-сказка-реальный продукт

2018



2019



2020

Сделано в кооперации. Разработано в России.

KISG 100

China

Russia

INNOPROM PLATFORM

Germany

HANNOVER MESSE

Шлюз промышленных данных

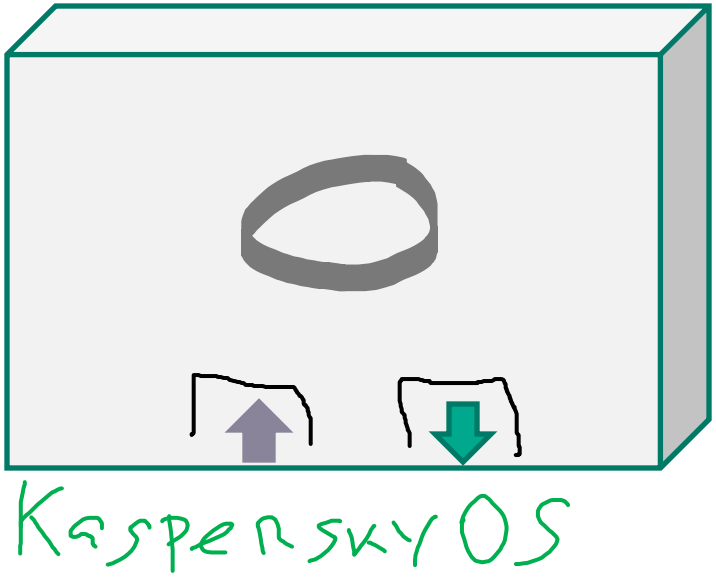
Почему он особенный?

реквизит на сцену...

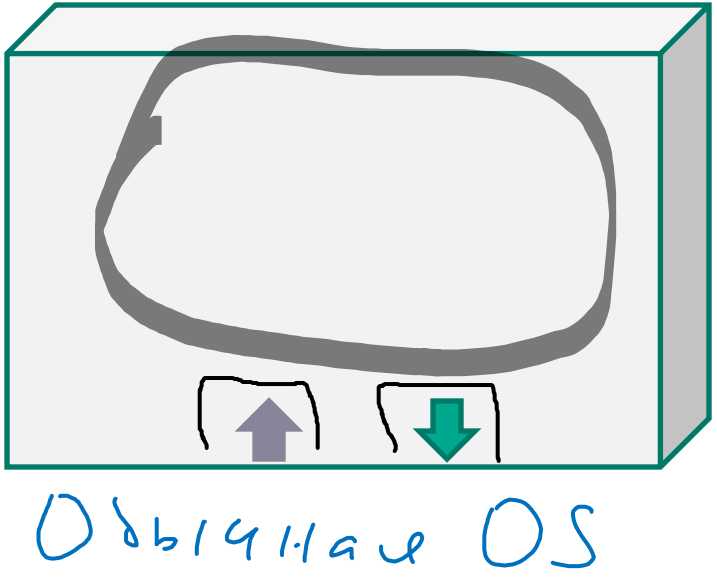
TCB Trusted Computing Base

... микро-ядро по-нашему

17к строк*



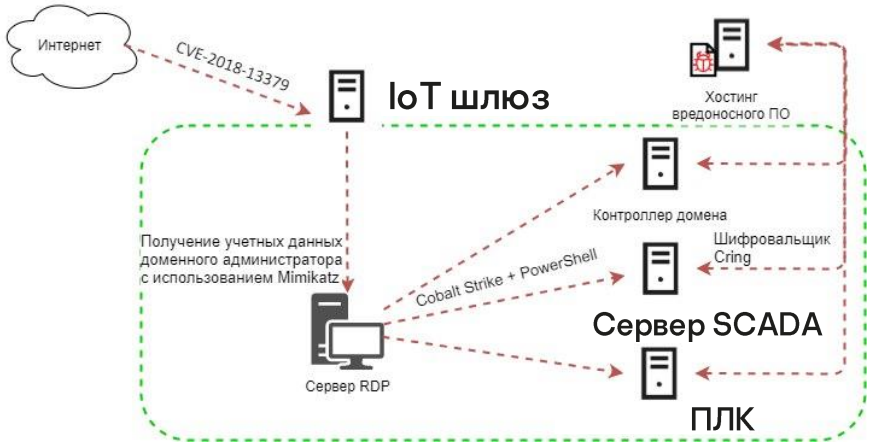
9М строк



*объем ядра ОС до компиляции

Потенциальный нарушитель. Сценарий 1.

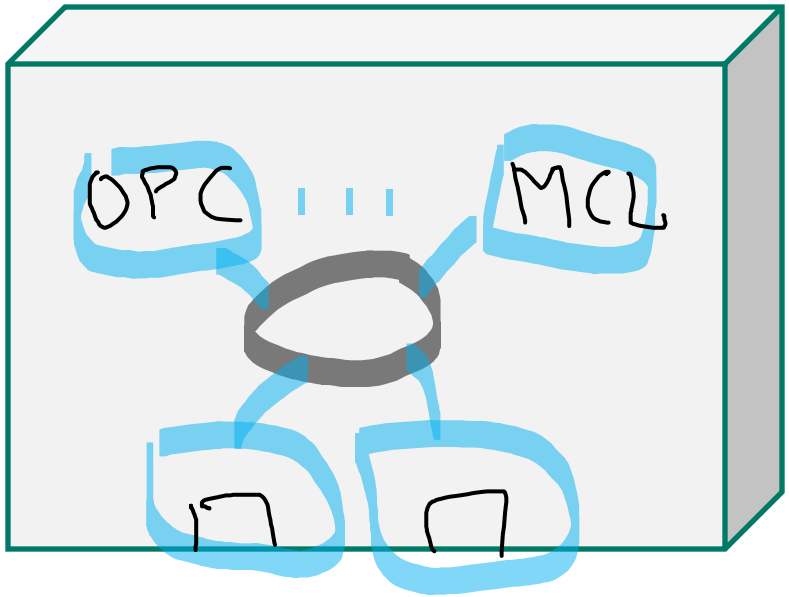
37,78%	Trojan-Downloader.Linux.NyaDrop.b
17,47%	Backdoor.Linux.Mirai.b
12,72%	HEUR:Backdoor.Linux.Mirai.b
9,76%	HEUR:Backdoor.Linux.Gafgyt.a
7,99%	Backdoor.Linux.Mirai.ba
4,49%	HEUR:Backdoor.Linux.Mirai.ba
2,23%	Backdoor.Linux.Gafgyt.bj
1,66%	HEUR:Trojan-Downloader.Shell.Agent.p
1,26%	Backdoor.Linux.Mirai.cn
0,73%	HEUR:Backdoor.Linux.Mirai.c

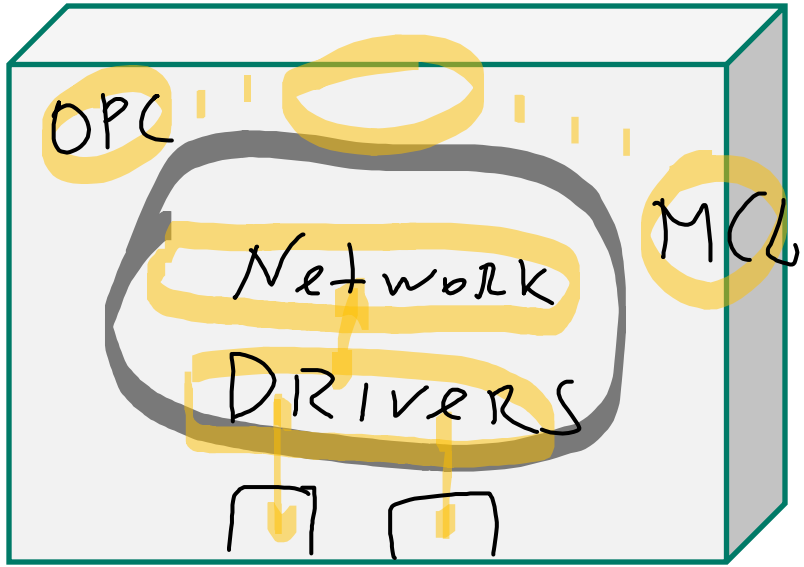


Kaspersky ICS CERT

MILS Multiple Independent Levels of Security

... разделяемые домены безопасности





20+ доменов

X

Потенциальный нарушитель. Сценарий 2.

Бизнес, 21 янв 2020, 10:54 | 168 775 | Поделиться

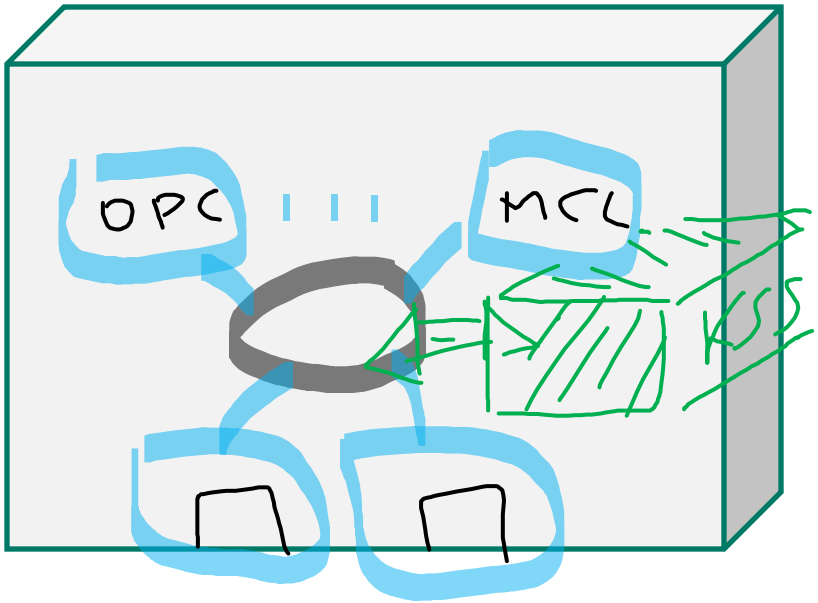
Сбербанк сообщил о мощнейшей в его истории DDoS-атаке

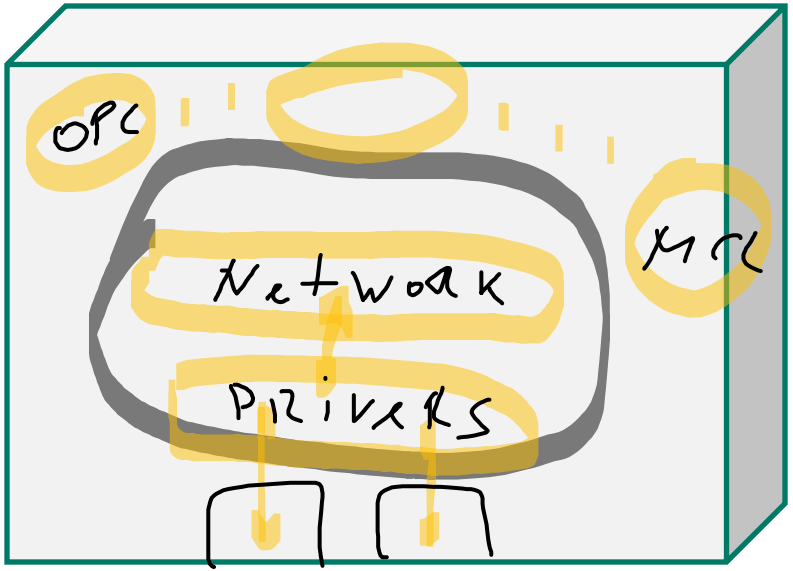
По словам зампреда Сбербанка, кибератаку провели 2 января, в ней задействовали устройства интернета вещей. В кредитной организации считают, что в 2020 году DDoS-атаки могут стать проблемой для многих компаний

https://www.rbc.ru/business/21/01/2020/5e26a8a69a79475cb4f039a5

FLASK Flux Advanced Security Kernel

... механизм управления политиками безопасности





X

KSS - политики

Потенциальный нарушитель. Сценарий 3.

cnews

24 июля 2020 09:59 | 24749 | ПОДЕЛИТЬСЯ

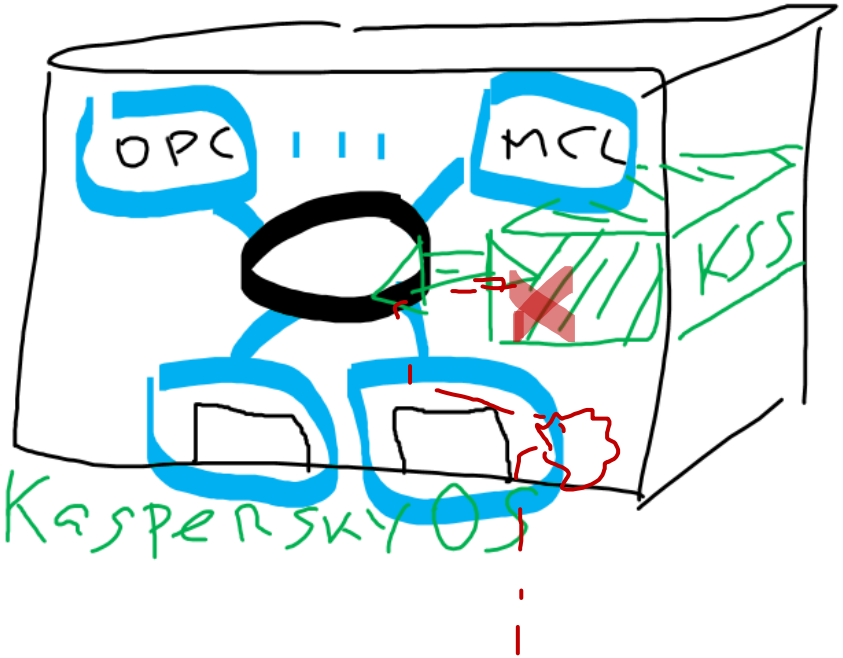
Тысячи устройств Garmin превратились в «кирпичи». Хакеры взломали ее системы и требуют миллионы долларов выкупа

https://www.cnews.ru/news/top/2020-07-24_tysyachi_ustrojstv_garmin_prevratilis

CNN politics The Biden Presidency Facts First US Elections Edition

First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers

https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html



Шлюзы KISG дают первую пользу

Дорожная карта цифровой трансформации

Дорожная карта цифровой трансформации

Особенности работы с облачными решениями

Основные компоненты решения:

- Шлюз данных на базе KasperskyOS
- Подключение по протоколу OPC UA с подготовкой данных для облачной IIoT-платформы
- Настройка облачного цифрового сервиса

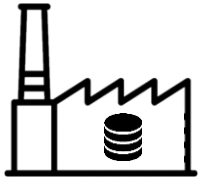
- ~~Локальное программное обеспечение~~
- ~~Дополнительные серверные мощности~~
- ~~Узкоспециализированные специалисты~~

SCADA и облако: отличительные особенности

SCADA – платформа для оперативного управления и интеграции производственных систем и инфраструктуры предприятия

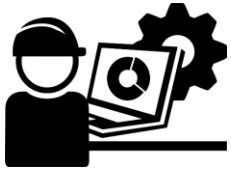
Сбор и обработка данных в режиме реального времени

Замкнутые контуры управления



Локальное хранение данных в

Функциональная безопасность



Контроль критических процессов

Выполнение спец./корп. требований

Облако – экосистема готовых приложений для запуска цифровых сервисов и построения кооперационных цепочек

Озеро данных

Экосистема готовых приложений

Совместная обработка данных из различных источников

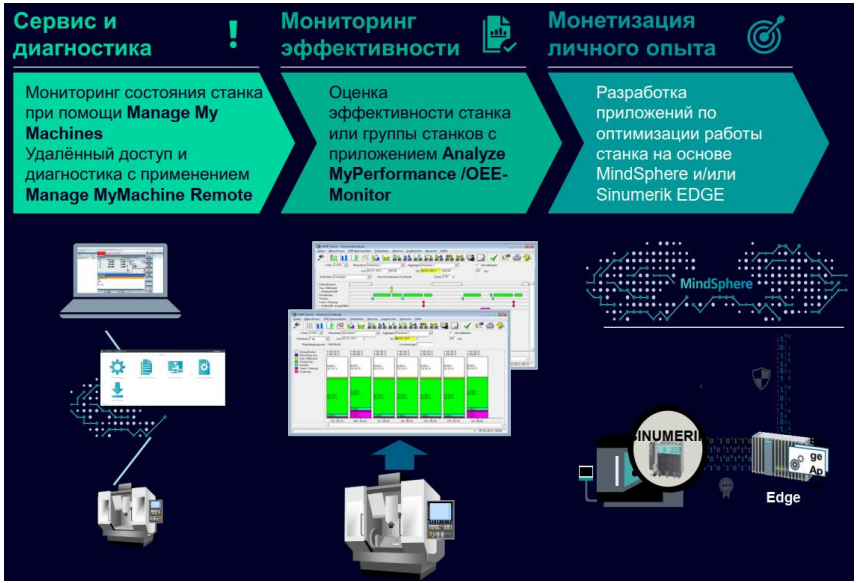
Цифровые сервисы и кооперационные цепочки

Использование моделей знаний (семантика, онтология)

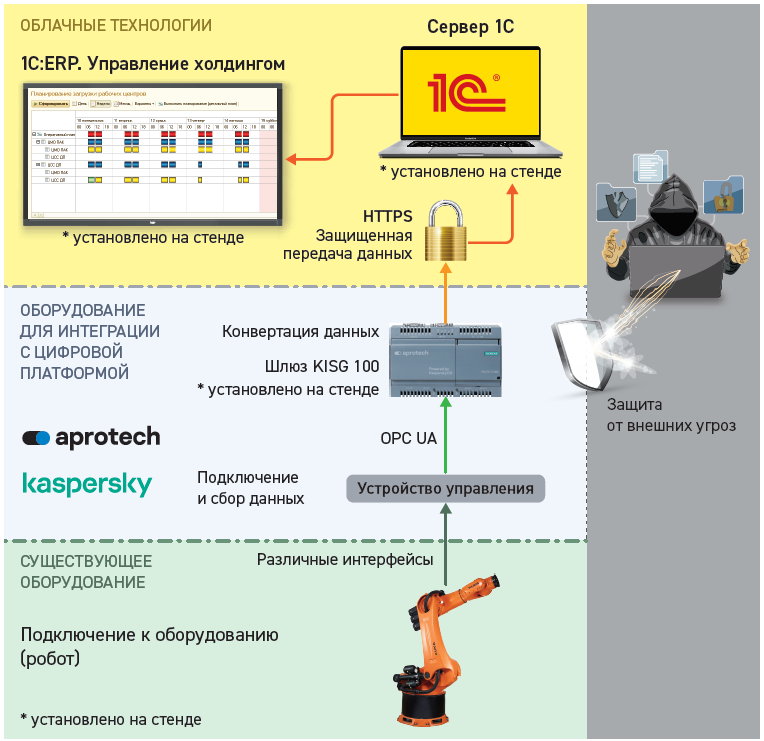
Наш кейс1. «Цифровой цех»

СТАН

Ростех и «Лаборатория Касперского» защитят «умные» станки от киберугроз



Наш кейс2. Объединение контура IIoT и ERP



В партнерстве с

CINIMEX KUKA

- Онлайн расчёт выполнения плана и зарплат
- Онлайн учёт простоя в минутах и рублях
- Контроль бережливого производства
- Детальный анализ выполнения программ

Отраслевой пример

Анализ надежности и производительности линий

Решение

- Сбор статистики и анализ поведения двигателей (создание моделей)
- Формирование пороговых значений для двигателей.

Результат

- Предсказание сбоев в двигателях и производственных линиях
- Эффективное планирование обслуживания
- Повышение качества и эффективности производства благодаря мониторингу в реальном времени

Thank you!

Добро пожаловать в цифровой мир кибериммунных устройств

Андрей Суворов

Максим Карпухин

aprotech

kaspersky